

**AFFIDAVIT IN SUPPORT OF  
SEIZURE WARRANT APPLICATION**

I, Bret Curtis, Special Agent, Federal Bureau of Investigation (“FBI”), being duly sworn, declare and state as follows:

**INTRODUCTION & PURPOSE OF THE AFFIDAVIT**

1. I make this affidavit in support of an application for the issuance of a seizure warrant to seize all cryptocurrency stored in the OKX<sup>1</sup> Account for User Identification Number (UIN) 259938855548010496 held in the name of SAY KYIN FEIN (**SUBJECT TARGET ACCOUNT**).

2. The **Subject Target Account** is believed to be the proceeds of violations of 18 U.S.C. § 1343 (Wire Fraud) and/or property involved in concealment money laundering in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (Concealment Money Laundering). For the court to authorize seizure of the Subject Target Account it must find probable cause to believe that: (1) the crimes of Wire Fraud and Concealment Money Laundering were committed; and (2) the Subject Target Account has a connection to those offenses in the manner specified by the below statutes authorizing forfeiture.

3. For the reasons set forth below, there is probable cause to believe the Subject Target Account has a connection to Wire Fraud and Concealment Money Laundering and are subject to **civil seizure and forfeiture** under the following forfeiture authorities:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) because the Subject Target Account is property, real or personal, which constitutes or are derived from proceeds traceable to a Wire Fraud. Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds from any offense constituting a “specified unlawful activity” as defined in 18 U.S.C. §

---

<sup>1</sup> OKX is cryptocurrency exchange. A cryptocurrency exchange is a platform used to buy and sell virtual currencies and allows users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa.

1956(c)(7), or a conspiracy to commit such offenses. A “specified unlawful activity,” as defined in Section 1956(c)(7), includes offenses listed in 18 U.S.C. § 1961(1). Section 1961(1) includes Wire Fraud violations.

- b. Pursuant to 18 U.S.C. § 981(a)(1)(A) because the Subject Target Account was involved in Concealment Money Laundering or is traceable to such property.
- c. Consequently, seizure of the Subject Target Account for civil forfeiture is authorized by 18 U.S.C. § 981(b).

4. For the reasons set forth below, there is probable cause to believe the Subject Target Account has a connection to Wire Fraud and Concealment Money Laundering and is subject to **criminal seizure and forfeiture** under the following forfeiture authorities:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) because the Subject Target Account is property, real or personal, which constitutes or are derived from proceeds traceable to Wire Fraud.
- b. Pursuant to 18 U.S.C. § 982(a)(1) because the Subject Target Account was involved in Concealment Money Laundering or are traceable to such property.
- c. Consequently, seizure of the Subject Target Account for criminal forfeiture is authorized by 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b).

5. Restraint of the Subject Target Account under 21 U.S.C. § 853(e) would likely not be sufficient to adequately protect them and preserve their availability for forfeiture and so a seizure warrant pursuant to 21 U.S.C. § 853(f) is necessary. Assets in a cryptocurrency exchange account are fungible and easily transferrable.

6. Although Rule 41(b) of the Federal Rules of Criminal Procedure provides that seizure warrants must be executed in the issuing district, other statutes authorize a magistrate to issue a warrant to seize property outside the district. Under 21 U.S.C. § 853(l), district courts have jurisdiction to authorize a criminal seizure warrant under 21 U.S.C. 853(f) “without regard to the location of any property which may be subject to forfeiture.” The same authority is granted for

civil forfeiture seizure warrants under 18 U.S.C. § 981(a) by 18 U.S.C. § 981(b)(3). OKX is in the Seychelles, but they accept U.S. warrants.

**BACKGROUND OF AFFIANT**

7. I am a Special Agent with the FBI in Salt Lake City, Utah. I have been an FBI Special Agent since February 22, 2004. In my capacity as a Special Agent with the FBI, I have conducted and participated in numerous official investigations into mail and wire fraud, money laundering and other financial and computer crimes as well as drug trafficking crimes. I am a graduate of the FBI Training Academy in Quantico, Virginia and have also attended advanced training classes in the areas of white-collar crime.

8. As an FBI Special Agent, I am familiar with the use of financial accounts by those who operate fraudulent schemes and the types of transactions reflected on financial account records. I am also familiar with the principles of tracing assets into and through financial accounts.

9. The facts set forth in this affidavit are based on my personal observations, my training and experience, my review of documents, interviews with witnesses, and others at FBI assisting with this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested seizure warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

**BACKGROUND ON CRYPTOCURRENCY**

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat (i.e. national currencies like the dollar, euro, yen, etc.) currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an

electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.<sup>2</sup> Cryptocurrency is not illegal in the United States.

b. Bitcoin<sup>3</sup> (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are

---

<sup>2</sup> Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

<sup>3</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

partially anonymous. And while it's not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transfers, trades, purchases, and other financial transactions. As of October 31, 2024, one bitcoin is worth approximately \$72,335.05 though the value of bitcoin is generally much more volatile than that of fiat currencies.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a

computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code<sup>4</sup> with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

f. Bitcoin “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.<sup>5</sup> Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often

---

<sup>4</sup> A QR code is a matrix barcode that is a machine-readable optical label.

<sup>5</sup> See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

g. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

#### **RELEVANT CRIMINAL STATUTES**

10. Title 18 U.S.C. § 1343 states:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures . . . for the purpose of executing such scheme or artifice.

11. Title 18 U.S.C. § 1956(a)(1)(B)(i) states:

Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

#### **FACTS SUPPORTING PROBABLE CAUSE**

12. This case involves the receipt of funds traceable to an online investment scam or scheme and the laundering of those proceeds into the SUBJECT TARGET ACCOUNT.

13. Online Investment Schemes. My investigation has revealed that fraudsters created and coordinated the use of fake online personas, and then used those fake online profiles or personas to engage in online chats, text messaging, and other forms of communication, with an unwitting victim to trick the victim into believing they were involved in real and lucrative investment opportunities. After gaining the victim's trust, the fraudsters then directed the victim to send their own personal funds to the fraudsters. Such frauds are also referred to as confidence scams.

#### **The Fraud Scheme**

14. Victim #1, age 33, resides in Draper, Utah and fell victim to an investment scam in which he believed he was sending money to cryptocurrency wallets to participate in a lucrative online investment involving cryptocurrency.

15. On November 21, 2024, Victim #1 met a person on Facebook calling herself Vivian Li. Li and Victim #1 developed a digital romantic relationship and communicated regularly using WhatsApp.

16. A Google image search revealed the photographs Li sent to Victim #1 of herself were really of a person named Nicole Wang Dan from Singapore. Through my training and experience, I have learned it is common for those involved in confidence scams to use the



photographs of attractive, sometimes famous individuals from other countries, to entice potential victims into a relationship.

17. Li told Victim #1 her aunt was a Harvard graduate of economics and said she developed a proven method to invest in cryptocurrency that assured large profits. Li sent Victim #1 a link to a platform at m.pyth-usvpu.top. On December 1, 2024, at Li's encouragement and invitation, Victim #1 began investing in cryptocurrency. Using his Crypto.com account, Victim #1 purchased \$500 worth of Tether (USDT).<sup>6</sup> At Li's direction, Victim #1 transferred the Tether to the following virtual wallet address: 3QH1qK2zSsejVLHMQRERgvLM7JgSRXirJy.

18. After transferring the money to the designated wallet, the m.pyth-usvpu.top platform showed a \$500 deposit and then large profits. On December 4, 2024, Victim #1 purchased \$10,000 worth of Bitcoin. At Li's direction, Victim #1 transferred the Bitcoin to the same virtual wallet address: 3QH1qK2zSsejVLHMQRERgvLM7JgSRXirJy. Again, the platform showed the \$10,000 deposit and subsequent large profits.

19. After making the \$10,000 deposit, Victim #1 asked to withdraw \$500 from the m.pyth-usvpu.top platform to prove to himself that the platform was legitimate. Victim #1 saw \$500 worth of cryptocurrency was transferred to his personal Crypto.com wallet. Victim #1 saw this transfer as proof the m.pyth-usvpu.top platform was legitimate, and he could withdraw money from the platform at will.

20. Victim #1 felt confident making a large deposit. On December 12, 2024, Victim #1 purchased \$37,887.28 of USDT using his Crypto.com wallet. At Li's direction, Victim #1 transferred the USDT to the following virtual wallet address: 0x7C858601e297529E4795f3AA985c3b3A8490222c.

21. On December 12, 2024, Victim #1 tried to withdraw \$37,887.28 USDT from the m.pyth-usvpu.top platform, but his request was denied. Victim #1 became suspicious and began to research Pyth. He learned Pyth is a legitimate cryptocurrency platform in Switzerland, but when

---

<sup>6</sup> USDT is a type of cryptocurrency on the Ethereum blockchain tied to the value of the US dollar.

he compared the m.pyth-usvpu.top platform Li provided him to the legitimate Pyth platform he saw they were similar, but not the same. Victim #1 realized the platform Li sent him was fraudulent. Victim #1 lost \$48,398.28 to the scam.

22. In my training and experience investigating cryptocurrency confidence scams, I have observed perpetrators utilize fake applications that appear to be fully functional and that lull victims through reports that give the appearance of profits like the m.pyth-usvpu.top platform.

### **Tracing of Victim #1's Funds into the SUBJECT TARGET ACCOUNT**

23. An FBI Digital Operations Specialist tracked the movement of the funds from the Victim to the Subject Target Account. The tracing is depicted below in Exhibit A. In tracing funds, investigators used a last in first out methodology. This method assumes that when dirty funds (last in) are deposited into an account/wallet then those dirty funds must be spent first (first out) even when subsequent "clean" funds are deposited. Once the entirety of the dirty funds are spent, then the clean funds are used for withdrawals. Courts have recognized the use of tracing methods to trace criminal proceeds including in *United States v. Banco Cafetero Panama*, 797 F.2d 1154 (2d Cir. 1986) (approving the use of accounting methods to trace criminal proceeds; government can choose the method).

24. Initially on December 12<sup>th</sup> 2024, Victim #1 sent 37,877.28 USDT to address 0x7c858601e297529e4795f3aa985c3b3a8490222c (222c). Twenty-four (24) minutes later the money was sent from address 222c to address 0x33b9d941ee5b2705c5d2fcdedff1227baea2dc1b9 (the Bitget deposit address).

25. The cryptocurrency sat in the Bitget account for around 20 minutes until 37,877.28 USDT was sent out to address TFgd6fFSSn8JLKCxoT17yrpz8DVDxcDCKh (DCKh). The funds sat in DCKh for around 7 hours until 81,287 USDT was sent to address TEFvQMRcvRRoqqswznQ499KTQ72tkoTQR (oTQR). The funds sat in oTQR for 5 days until

on December 18, 2024, when they were sent to OKX deposit address

TDL0NM7MX9QU8DTae6TVbinM4zQ7QorYUz (The OKX Deposit Address).

26. The OKX Deposit Address belongs to the SUBJECT TARGET ACCOUNT. On January 8, 2025, OKX records showed the following cryptocurrency balance in the SUBJECT TARGET ACCOUNT:

OKX UID	Account Holder Name	Approximate Balance (USD equivalent)
259938855548010496	SAY KYIN FEIN	\$108,737.56

27. Based on my training and experience, I am aware that individuals engaged in cryptocurrency confidence scams will sometimes move cryptocurrency obtained from the fraud through numerous addresses, cryptocurrency services and exchanges, and accounts to commingle it for the purpose of concealing the nature, source, location, ownership, or control of the fraud proceeds. The transfers in this case appear to fit this paradigm and do not have any indication of legitimate economic character or purpose.

**CONCLUSION**

28. Based on the above, there is probable cause to believe that the crimes of Wire Fraud and Money Laundering have occurred and that all cryptocurrency in the SUBJECT TARGET ACCOUNT is either proceeds of wire fraud and/or property involved in concealment money laundering. Accordingly, the SUBJECT TARGET ACCOUNT is subject to seizure and forfeiture under the authorities described above.

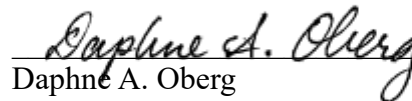
I swear, under penalty of perjury, that the foregoing is true and correct.



---

Bret Curtis, Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me telephonically this  
21st day of January, 2025.



---

Daphne A. Oberg  
United States Magistrate Judge

EXHIBIT A

